IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

UNITED STATES OF AMERICA, Plaintiff, v. HONGJIN TAN, Defendant.	Case No. 19-CR-9-GKF

OPINION AND ORDER

Before the court is the Motion to Suppress [Doc. 49] of defendant Hongjin Tan. He seeks to suppress all evidence obtained under three search warrants, which, he contends, lack the particularity required by the Fourth Amendment. For the following reasons, the motion is granted in part and denied in part.

I. Background

A. Charges against Mr. Tan

On December 20, 2018, the government filed a criminal complaint against Mr. Tan, along with a supporting affidavit signed by James Judd, a Special Agent with the Federal Bureau of Investigation. [Doc. 1]. According to the affidavit, Mr. Tan is a citizen of The People's Republic of China. [Doc. 1, p. 2 ¶ 7]. In April 2017, he was hired as a research engineer at a large international corporation located in Oklahoma, which the affidavit refers to as "Company A." [*Id.*, p. 2 ¶¶ 3, 7]. Citing information provided by Company A, the affidavit further states that, on December 12, 2018, Mr. Tan contacted his supervisor, advised he was resigning from Company A, and gave two weeks' notice. [*Id.*, p. 3 ¶ 10]. He told his supervisor that he did not currently have a job offer, but was negotiating with companies in China. [*Id.*].

Mr. Tan's resignation prompted Company A to revoke his access to company systems and to conduct a review of his computer activity. [*Id.*, p. 3 ¶ 11]. That review revealed that Mr. Tan had accessed hundreds of files, including research reports. [*Id.*, p. 3 ¶ 12]. These files included information that Company A considers to be trade secrets and outside the scope of Mr. Tan's employment. [*Id.*]. The review also revealed Mr. Tan downloaded restricted files to a personal thumb drive. [*Id.*]. Based on that information, Company A officials escorted Mr. Tan from Company A property and barred him from returning. [*Id.*, p. 3 ¶ 13].

Later that day, Mr. Tan sent a text message to his supervisor stating that he had "a memory disk" containing "lab data" and "papers/reports." [*Id.*, p. 4 ¶ 15]. Mr. Tan inquired about the best way of handling the information and whether he could still read the papers/reports. [*Id.*]. At his supervisor's request, Mr. Tan returned the flash drive to Company A. [*Id.*, p. 4 ¶¶ 16–17]. Upon reviewing the drive, Company A determined that it contained research documents in deleted and undeleted files that would have a tremendous impact to Company A in terms of technological and economic loss if they were shared or given to a competing company. [*Id.*, p. 4 ¶ 18]. The review further revealed that the deleted files had been deleted on December 11, 2018, the day before Mr. Tan's resignation. [*Id.*, p. 4 ¶ 19]. The affidavit alleges additional facts pertaining to Mr. Tan's contacts with a Chinese competitor of Company A, records of Mr. Tan's recent travel to China, and Company A's protection of its trade secrets. [*Id.*, pp. 5–8].

On January 16, 2019, a grand jury returned an indictment charging Mr. Tan with three counts: (1) theft of trade secrets, in violation of 18 U.S.C. § 1832(a)(1); (2) unauthorized transmission of trade secrets, in violation of 18 U.S.C. § 1832(a)(2), and (3) unauthorized possession of trade secrets, in violation of 18 U.S.C. § 1832(a)(3). [Doc. 18].

B. Search Warrants

On December 19, 2018, the government applied for a warrant to search Mr. Tan's residence and vehicle in relation to an alleged violation of 18 U.S.C. § 1832(a)(2). [Doc. 55-1, p. 6–20]. The application was assigned case number 18-mj-175-JFJ. Special Agent Judd swore to and signed the application and a supporting affidavit before United States Magistrate Judge Jodi F. Jayne, who issued the warrant that day. [*Id.*, pp. 2–6, 14].

On January 3, 2019, the government applied for a warrant to search two of Mr. Tan's Yahoo e-mail accounts in relation to an alleged violation of 18 U.S.C. §§ 1832(a) and 1030(a)(1). [Doc. 55-2, pp. 7–20]. The application was assigned case number 19-mj-2-PJC. United States Magistrate Judge Paul J. Cleary issued the warrant that day. [*Id.*, pp. 2–6].

On February 11, 2019, the government applied for a warrant to search Mr. Tan's Gmail account in relation to an alleged violation of 18 U.S.C. §§ 1832(a) and 1030(a)(1). [Doc. 55-3, pp. 7–20]. The application was assigned case number 19-mj-37-FHM. United States Magistrate Judge Frank H. McCarthy issued the warrant that day. [*Id.*, pp. 2–6].

After Mr. Tan filed the instant motion to suppress, the government filed a written response, and Mr. Tan filed a reply. [Doc. 50; Doc. 60]. On May 17, 2019, this court conducted an evidentiary hearing on the motion. *See* [Doc. 79]. During the hearing, the government called five witnesses to testify: James Judd, Shannon Clark, Brian Dean, Steve Carnivale, and Jeremy Sykes. All five are special agents with the FBI.

II. Legal Standards

A. Particularity Requirement

The Fourth Amendment of the Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause,

> supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Thus, a search warrant must particularly describe the persons or things that the government may seize. This requirement "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

In recent decades, the Tenth Circuit has extensively discussed the particularity requirement in the context of searches of digital files. *See, e.g.*, *United States v. Loera*, 923 F.3d 907 (10th Cir. 2019); *United States v. Russian*, 848 F.3d 1239, 1245 (10th Cir. 2017); *United States v. Christie*, 717 F.3d 1156, 1164 (10th Cir. 2013); *United States v. Burke*, 633 F.3d 984, 992 (10th Cir. 2011); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009); *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005); *United States v. Riccardi*, 405 F.3d 852, 861 (10th Cir. 2005); *United States v. Campos*, 221 F.3d 1143, 1148 (10th Cir. 2000); *United States v. Carey*, 172 F.3d 1268, 1272 (10th Cir. 1999). "The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important." *Otero*, 563 F.3d at 1132.

"[W]arrants for computer searches must affirmatively limit the search to evidence of specific federal crimes or specific types of material." *Burke*, 633 F.3d at 992 (quoting *Riccardi*, 405 F.3d at 862). A warrant should enable "the searcher to reasonably ascertain and identify the things authorized to be seized." *Cooper*, 654 F.3d at 1126 (quoting *Riccardi*, 405 F.3d at 862).

As a general rule, reviewing courts "should interpret warrants in a commonsense and realistic fashion, rather than a hypertechnical manner." *United States v. Sells*, 463 F.3d 1148, 1156 (10th Cir. 2006) (internal quotation marks omitted). In addition, "whether a search warrant is

sufficiently particular depends in part on the nature of the crimes being investigated." *Cooper*, 654 F.3d at 1127. "Even a warrant that describes the items to be seized in broad or generic terms may be valid when the description is as specific as the circumstances and the nature of the activity under investigation permit." *Riccardi*, 405 F.3d at 862 (quoting *United States v. Leary*, 846 F.2d 592, 600 (10th Cir. 1988)).

The Tenth Circuit recently observed that its "electronic search precedents demonstrate a shift away from considering what digital location was searched and toward considering whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant." *Loera*, 923 F.3d at __.[1] This shift in focus "is necessary in the electronic search context because search warrants typically contain few—if any—restrictions on where within a computer or other electronic storage device the government is permitted to search." *Id.* The Tenth Circuit thus prescribed an "ex post assessment of the propriety of a government search" in this context. *Id.* The court described the relevant principles for the *ex post* assessment as follows:

> In all cases, the ultimate test is the one mandated by the Fourth Amendment: whether the search was "reasonable" under the circumstances. In the case of a computer search, "reasonableness" requires officers to take into account the flexibility of computers and the multiple configurations to which they may be adapted. As the computer search continues and as the executing officer obtains more information about how a suspect used his computer, that too may inform the reasonableness of the continuing search.

Id. at __.

B. Good-Faith Exception to the Exclusionary Rule

"Even if a warrant fails to satisfy the Fourth Amendment's particularity requirement, the exclusionary rule should not be applied to suppress evidence obtained by officers acting in

[1] Reporter pagination is not yet available.

objectively reasonable reliance on a search warrant issued by a detached and neutral magistrate judge that is ultimately deemed invalid." *Russian*, 848 F.3d at 1246 (citing *United States v. Leon*, 468 U.S. 897, 922 (1984)). Importantly, "the exclusionary rule is not an individual right." *Herring v. United States*, 555 U.S. 135, 141 (2009). The rule's purpose is to deter police misconduct, and "the suppression of evidence obtained pursuant to a warrant should be ordered only in the unusual cases in which exclusion will further the purposes of the exclusionary rule." *Riccardi*, 405 F.3d at 863 (citing *Leon*, 468 U.S. at 918). The rule applies only where it results in appreciable deterrence, and "the benefits of deterrence outweigh the costs." *Herring*, 555 U.S. at 141.

III. Discussion

The court will first address the warrant to search Mr. Tan's residence and his vehicle, and will then address the warrants to search his e-mail accounts.

A. Search Warrant for Mr. Tan's Residence and Vehicle

1. Particularity

Mr. Tan argues that the warrant to search his residence and vehicle was invalid because it failed to describe with particularity the things to be seized. In the space set aside for a description of the property to be seized, the warrant refers to Attachments A and B. [Doc. 55-1, p. 2]. But those attachments describe the properties to be searched, not the items to be seized. [*Id.*, pp. 4–5]. "In other words, the warrant did not describe the items to be seized *at all*." *Groh v. Ramirez*, 540 U.S. 551, 558 (2004). The court therefore agrees that the warrant failed to meet the Fourth Amendment's particularity requirement. *See id.*

The government argues that the warrant was valid because the affidavit supporting the warrant application incorporated Attachment C, which described the property to be seized. [Doc. 55-1, pp. 17–20]. But the government's argument fails because "[t]he Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents." *Groh*, 540

U.S. at 557. The government concedes that "[t]he application and search warrant documents do not reference Attachment C on the face of the documents." [Doc. 55, p. 11]. Thus, the warrant to search Mr. Tan's residence and vehicle was invalid.

2. Good-Faith Exception

Although the warrant was invalid, the court may consider whether the good-faith exception to the exclusionary rule applies. Mr. Tan contends the government waived any argument that the good-faith exception applies because it did not raise the issue in its written response. However, the court will consider the issue because the government raised it during the suppression hearing. *See United States v. Solis*, No. CR 13-3895 MCA, 2015 WL 13651018, at *7 (D.N.M. Mar. 20, 2015) (government did not waive good-faith exception where raised at hearing), *report and recommendation adopted*, No. CR 13-3895 MCA, 2015 WL 13651019 (D.N.M. Dec. 23, 2015).

Several factors lead the court to conclude that the FBI agents' reliance on the warrant was reasonable. First, due to the particular circumstances of this case, the government prepared the warrant application and executed the search under time pressure. The government commenced its investigation after receiving a call on December 13, 2018, from a representative of Company A reporting a theft of trade secrets. [Doc. 1, p. 3]. Although this case involves technical factual issues, the government was obliged to react promptly due to Company A's concerns of theft of trade secrets and concerns that Mr. Tan posed a flight risk because he is not a U.S. citizen and had preexisting plans to leave the country. [Doc. 53-1, p. 8; Doc. 79, pp. 12:21–13:3].

Second, the affidavit supporting the warrant application expressly incorporated "Attachment C," which described the items to be seized. "Although a warrant application or affidavit cannot save a warrant from facial invalidity, it can support a finding of good faith . . . ." *Russian*, 848 F.3d at 1246. Attachment C limited the property to be seized to records and equipment relating to violations of 18 U.S.C. § 1832(a)(2). FBI agents did not prepare the warrant

itself, *see* [Doc. 79, p. 24:4–14], and the record contains no evidence that the failure of the warrant to reference Attachment C was anything other than a drafting mistake.

Third, in addition to signing the warrant itself, the magistrate judge signed the warrant application and the affidavit. [Doc. 55-1, pp. 6, 14]. Moreover, the magistrate judge specifically reviewed and modified Attachment C, indicating that she intended Attachment C to limit the scope of the warrant. [Doc. 55-1, p. 17; Doc. 79, pp. 13:20–15:23]. "The magistrate judge's approval of the application and affidavit . . . further supports the objective reasonableness of [the FBI agents'] reliance on the warrant." *Russian*, 848 F.3d at 1247.

Fourth, agents with the FBI Evidence Response Team used Attachment C to guide them in their search of the residence and vehicle when executing the search warrant. [Doc. 79, pp. 29:2–30:18, 41:3–12]. The packet given to search team members before the search included Attachment C, which was also included among the documents left at the residence at the conclusion of the search. [Doc. 79, pp. 31:11–25, 33:13–18].

"Finally, excluding the challenged evidence would not serve the underlying purpose of the exclusionary rule." *Russian*, 848 F.3d at 1247. The Supreme Court has explained:

> When the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs. But when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way.

Davis v. United States, 564 U.S. 229, 238 (2011) (internal quotation marks and citations omitted). Upon consideration of the facts presented here, the court finds and concludes that the agents acted with an objectively reasonable good-faith belief that their conduct was lawful, and, at most, their conduct merely rises to simple, isolated negligence.

Mr. Tan argues that, even taking into account Attachment C, the warrant was overbroad or the execution of the search was improper because the government seized or imaged the entirety of certain electronic devices. The court finds this argument unpersuasive. Because the investigation involved evidence that Mr. Tan used a computer and other electronic media in the commission of the suspected criminal acts, the government reasonably sought to conduct an extensive search of various types of electronic media in his possession. *See Cooper*, 654 F.3d at 1127 ("[W]hether a search warrant is sufficiently particular depends in part on the nature of the crimes being investigated."). "Given the numerous ways information is stored on a computer, openly and surreptitiously, a search can be as much an art as a science." *Brooks*, 427 F.3d at 1252. The possibility that relevant documents might require translation from the Chinese language further complicated the search here. Under the circumstances, it would have been "unrealistic to expect [the] warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods," as that process needed to remain dynamic. *Burgess*, 576 F.3d at 1093.

Furthermore, "[c]omputers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location." FED. R. CRIM. P. 41, Advisory Committee Notes to 2009 Amendments; *see generally United States v. Ganias*, 824 F.3d 199, 215–17 (2d Cir. 2016). It was therefore reasonable for the government to seize or copy the entire storage media and review it later to determine what electronically stored information fell within the scope of the warrant. Notably, this is not "a situation where a police officer executing a warrant to search an electronic storage device for evidence of one crime discovers evidence of other criminal

activity." *Cf. Loera*, 923 F.3d at __. Here, the testimony reflects that the agents reasonably directed their search at uncovering evidence of the crime specified in Attachment C.

The court therefore concludes that the good-faith exception to the exclusionary rule applies, and the motion to suppress is denied with respect to evidence obtained pursuant to the warrant to search Mr. Tan's residence and his vehicle.

B. Search Warrants for Mr. Tan's E-mail Accounts

1. Particularity

Unlike the warrant to search Mr. Tan's residence and vehicle, the two warrants to search his e-mail accounts each expressly referenced and attached an "Attachment B" that described the items to be disclosed by the e-mail service provider and the items to be seized by the government. [Doc. 49-2; Doc. 49-3]. Both warrants limited the information to be seized by the government to that which "constitutes fruits, evidence, and instrumentalities of violations of" 18 U.S.C. §§ 1832(a) and 1030(a)(1). [Doc. 49-2, p. 6; Doc. 49-3, p. 6].

The warrants were not general warrants because they restricted the scope of the search to information, from an approximately two-year period, related to the particular federal crimes identified in Attachment B. *Cf. Brooks*, 427 F.3d at 1253 (approving "warrant that authorized officers to search through computer files for particular items specifically related to child pornography"). Because the investigation involved evidence that Mr. Tan used a computer and other electronic media to store and transmit digital files containing trade secrets, as well as evidence that he had used his personal e-mail to transmit a potentially incriminating agreement with a Chinese company, *see* [Doc. 79, pp. 45:16–46:3], the government reasonably sought to conduct an extensive search of Mr. Tan's electronic communications.

Mr. Tan argues that the warrants violated the Particularity Clause because they required Yahoo and Google to disclose *all* e-mails within his accounts for a specified timeframe. Special

Agent Sykes testified that law enforcement officers typically interact with technology companies such as Yahoo and Google regarding search warrants through an online portal, and the companies usually provide all information within a given date range. [Doc. 79, pp. 64:13–65:12]. He further testified that he did not believe those companies would take the time to sift through e-mails and use search terms to provide e-mails only in reference to specific subject matters. [Doc. 79, p. 64:13–22]. Counsel for Mr. Tan did not dispute that the technology companies would not perform the searches for law enforcement. [Doc. 79, p. 84:8–12]. It was thus reasonable for the warrant to require the companies to disclose all e-mails within the specified timeframe. *Cf. Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.").

In reviewing Mr. Tan's e-mails, the FBI developed and employed a list of search terms and targeted dates. [Doc. 79, pp. 52:15–54:12]. Based on the agents' testimony at the suppression hearing, the court finds that the search process was "reasonably directed at uncovering the evidence specified in the search warrant." *Loera*, 923 F.3d at __. The court concludes that the warrants described the information to be seized with sufficient particularity under the circumstances, and that the agents reasonably conducted their searches within the bounds set by the warrants.

2. Good-Faith Exception

Even if the warrants to search Mr. Tan's e-mail accounts were constitutionally deficient, the good-faith exception would apply. An objectively reasonable FBI agent acting in good faith could have read the warrants as restricting the scope of any search in a manner sufficient to satisfy the Fourth Amendment's particularity requirement. In light of the Tenth Circuit's past approval of similar warrants, "suppression cannot follow." *Christie*, 717 F.3d at 1165.

3. Attorney-Client Communications

Mr. Tan objects that the government seized privileged communications between Mr. Tan and his counsel. [Doc. 49, p. 11]. The parties have provided the court with little information about the nature and quantity of the communications at issue, but they were apparently contained within one of Mr. Tan's Yahoo e-mail accounts. [Doc. 79, p. 53:7–15].

Special Agent Carnivale testified that, in the course of reviewing e-mails from the Yahoo account using searches based on specific dates, he came across an e-mail between Mr. Tan and counsel unrelated to this case. [Doc. 79, p. 54:13–22]. He further testified that, as soon as he figured out what the e-mail was, he stopped reading it and from then on skipped over e-mails with the same individual. [Doc. 79, pp. 54:25–55:2]. Special Agent Sykes testified that, in the course of reviewing Mr. Tan's e-mails, he "did not run across any e-mails that were attorney-client privileged." [Doc. 79, p. 68:11–12]. He first learned about potentially privileged e-mails from counsel for the government after defense counsel filed a motion with the court. [Doc. 79, p. 68:12–19]. After learning of the concern, Special Agent Sykes searched the attorney's name—which Agent Carnivale had previously encountered—in the Yahoo account and highlighted the results as e-mails not to look at. [Doc. 79, pp. 68:20–69:7]. Counsel for the government represented to the court that she has not reviewed any attorney-client privileged communications obtained from Mr. Tan's e-mails. [Doc. 79, pp. 5:19–6:1]. Counsel further represented that the government has guided its process by specific search terms relevant to this prosecution, and, to her knowledge, those search terms have not produced any attorney-client communications. [Doc. 79, p. 6:1–6:9].

The government has represented that the attorney-client privileged e-mails at issue are unrelated to this case and have not been reviewed by the agents or prosecutors involved. It appears that the government has handled its inadvertent seizure of attorney-client communications in a reasonable manner. Nevertheless, out of an abundance of caution, the court grants the motion to

suppress with respect to any privileged attorney-client communications seized by the government in executing the warrants to search Mr. Tan's e-mail accounts, and the government is prohibited from reviewing or otherwise using such communications in connection with this case.

IV. Conclusion

WHEREFORE, defendant's Motion to Suppress [Doc. 49] is granted in part and denied in part. The motion is granted with respect to any privileged attorney-client communications seized by the government in executing the warrants to search Mr. Tan's e-mail accounts and is otherwise denied.

IT IS SO ORDERED this 31st day of May, 2019.

GREGORY K. FRIZZELL
UNITED STATES DISTRICT JUDGE